A new method to represent the inverse map as a composition of quadratics in a binary finite field

Florian Luca[1,2], Santanu Sarkar[3], Pantelimon Stănică[4]

[1] School of Mathematics, University of the Witwatersrand,
Private Bag X3, Wits 2050, Johannesburg, South Africa; and
[2] Centro de Ciencias Matemáticas, UNAM,
Morelia, Mexico; Florian.Luca@wits.ac.za,
[3] Department of Mathematics, Indian Institute of Technology Madras,
Sardar Patel Road, Chennai TN 600036, INDIA; santanu@iitm.ac.in,
[4] Applied Mathematics Department, Naval Postgraduate School,
Monterey 93943, USA; pstanica@nps.edu

June 24, 2023

1 Introduction

Carlitz [1] showed that all permutation polynomials over $\mathbb{F}_q$, where $q > 2$ is a power of a prime, are generated by the special permutation polynomials x^{q-2} (the inversion) and $ax + b$ (affine functions, where $0 \neq a, b \in \mathbb{F}_q$). The smallest number of inversions in such a decomposition is called the *Carlitz rank*.

Here, we ask whether the inverse in $\mathbb{F}_{2^n}$ (the finite field of dimension n over the two-element prime field $\mathbb{F}_2$) can be written as a composition of quadratics (and suggest an extension allowing quadratics and cubics). That is, we ask if there are integers $r \geq 1$ and $a_1 \geq 0, \ldots, a_r \geq 0$ such that $-1 \equiv \prod_{i=1}^{r}(2^{a_i} + 1) \pmod{2^n - 1}$. Nikova, Nikov, Rijmen [8] proposed an algorithm to find such a decomposition. Via Carlitz [1], they were able to use the algorithm and show that for $n \leq 16$ any permutation can be decomposed in quadratic permutations, when n is not multiple of 4 and in cubic permutations, when n is multiple of 4. Petrides [9], in addition to a theoretical result, which we will discuss below, improved the complexity of the algorithm and presented a computational table of shortest decompositions for $n \leq 32$, allowing also cubic permutations in addition to quadratics. Here, we extend Petrides' result, as well as we propose a number theoretical approach, which allows us to cover easily all (surely, odd) exponents up to 100, at least, with weight 2 factorizations (in the full paper we will cover up to n a few hundred). Our method is based on some hard number theoretical conjectures we propose, which allow us some inferences in our algorithmic approach. The algorithm easily extends the table of Nikova, Nikov, Rijmen [8] and Petrides [9] that covered the mentioned factorizations up to $n = 32$.

2 Our results

Let ν_2 be the 2-valuation, that is, the largest power of 2 dividing the argument. We start with a proposition, extending one of Petrides' results [9], which stated that if n is an odd integer and $\frac{n-1}{2^{\nu_2(n-1)}} \equiv$

$2^k \pmod{2^n-1}$, for some k, then,

$$
\begin{aligned}
2^n-2 &= 2\left(\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}}\right)^{2^{\nu_2(n-1)}}-1\right) = 2\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}}-1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right)\\
&\equiv 2\left(2^{2^k}-1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right) = 2\prod_{j=0}^{k-1}\left(2^{2^j}+1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right).
\end{aligned}
$$

This implies, via Carlitz [1], that for all odd integers (coined *good integers*, with the counterparts named *bad integers* in [6]) satisfying the congruence $\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k \pmod{2^n-1}$, one can decompose any permutation polynomial in $\mathbb{F}_{2^n}$ into affine and quadratic power permutations.

The smallest odd positive integer that is not *good* is $n=7$. We note however that in that case $2^7-2 = 2(2^6-1) = 2(2^2-1)(2^4+2^2+1) = 2(2+1)(2^4+2^2+1)$, and so, any permutation in $\mathbb{F}_{2^7}$ can be decomposed into affine, quadratic and cubic permutations. We are ready to generalize this observation.

Theorem 1. *Let n be an odd integer satisfying $\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k 3^s \pmod{2^n-1}$, for some non-negative integers r,s. Then, the inverse power permutation in $\mathbb{F}_{2^n}$ has a decomposition into affine, quadratic and cubic power permutations of length $k+s+\nu_2(n-1)$.*

Proof. We use the difference of cubes factorization, $a^3-b^3=(a-b)(a^2+ab+b^2)$, and write

$$
\begin{aligned}
2^n-2 &= 2\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}}-1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right) \equiv 2\left(2^{2^k3^s}-1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right)\\
&= 2\left(2^{2^k3^{s-1}}-1\right)\left(2^{2^{k+1}3^{s-1}}+2^{2^k3^{s-1}}+1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right)\\
&\cdots\cdots\cdots\cdots\\
&= 2\left(2^{2^k}-1\right)\prod_{j=0}^{s-1}\left(2^{2^{k+1}3^j}+2^{2^k3^j}+1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right)\\
&\equiv 2\prod_{j=0}^{k-1}\left(2^{2^j}+1\right)\prod_{j=0}^{s-1}\left(2^{2^{k+1}3^j}+2^{2^k3^j}+1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}}+1\right).
\end{aligned}
$$

The claim is shown. □

Example 1. *It is natural to investigate the counting function $\mathcal{B}(x)$ of* superbad integers *(that is, integers n such that $\frac{n-1}{2^{\nu_2(n-1)}} \not\equiv 2^k3^s \pmod{2^n-1}$), with $\mathcal{B}(x) = \{n \le x : n \text{ is superbad}\}$, or the complement $\mathcal{A}(x) = \{n \le x : \frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k3^s \pmod{2^n-1}\}$. As an example, $|\mathcal{B}(50)| = 16$, more precisely, $\mathcal{B}(50) = \{1,2,3,4,5,7,9,10,13,17,19,25,28,33,37,49\}$ (Petrides [9] noted that 25 integers up to 50 are bad, so our extension surely prunes the integers better).*

Let $p \ge 3$ be prime, $N := N_p = 2^p-1$. It is known that if $q \mid N_p$, then $q \equiv 1 \pmod{p}$. We ask if we can say anything about the number of distinct prime factors $\omega(N_p)$ of N_p. Recall that, via Mihailescu's theorem (which solves Catalan's conjecture from 1844) [5], we know that 2^p-1 is not a (nontrivial) prime power, if $p \ge 3$. In general, we propose the following conjecture.

Conjecture 1. *There exists p_0 such that for $p > p_0$, $\omega(N_p) < 1.36 \log p$.*

Similar type of heuristics regarding lower bounds for $\Omega(2^n-1)$ and $\omega(2^n-1)$ can be found in [3] and [4]. Conjecture 1 is based on statistical arguments originating from sieve methods. It is shown in [2, Exercise 04] that for fixed $\delta>0$ we have

$$\#\{n \le x : \omega(n) \ge (1+\delta)\log\log x\} \ll_\delta \frac{x}{(\log x)^{Q(\delta)}},$$

where $Q(\delta) := (1+\delta)\log((1+\delta)/e)+1$. We apply such heuristics to $N_p = 2^p-1$. Note that if $q \mid N_p$, then $2^p \equiv 1 \pmod q$. In particular, $\left(\dfrac{2}{q}\right)=1$, so $q\equiv \pm 1 \pmod 8$. Using a similar approach as in [2, Exercise 04] we can infer that the probability that a number having only prime factors congruent to $\pm 1 \pmod 8$ to have more than $1.36\log\log n$ distinct prime factors is $O\left(\frac{1}{(\log n)^{1.00008}}\right)$. Applying this to N_p, we get $O\left(\frac{1}{(\log(2^p-1))^{1.0008}}\right) \ll \frac{1}{p^{1.0008}}$, and since the series $\sum_{p\ge 3}\frac{1}{p^{1.0008}}$ is convergent, we are led to believe that there are at most finitely many prime numbers p such that $\omega(N_p)\ge 1.36\log p$. Perhaps infinitely often $\omega(N_p)\ge 2$. For example, this is the case if $p\equiv 3 \pmod 4$ is such that $q=2p+1$ is prime. Indeed, then 2 is a quadratic residue modulo q so $2^{(q-1)/2}\equiv 1 \pmod q$, showing that $q\mid N_p$. Since N_p is never a perfect power, in particular it cannot be a power of q, we get the desired conclusion that $\omega(N_p)\ge 2$. The next conjecture is proposed based upon some results of Murata and Pomerance, under the Generalized Riemann Hypothesis (GRH).

Conjecture 2. *There exists p_0 such that if $p>p_0$, then N_p is squarefree.*

So, assuming Conjecture 1 and 2, let $N_p := q_1\cdots q_k$ for some distinct primes $q_1,\ldots,q_k$ with $k\le 1.36\log p$. We take numbers of the form 2^a+1 with an odd $a\in[5,p-2]$. We want to compute $\left(\frac{2^a+1}{2^p-1}\right)$, and use a method by Rotkiewicz [10]. Precisely, we write the Euclidean algorithm with even quotients and signed remainders:

$$\begin{array}{rcl}
p &=& (2k_1)a+\varepsilon_1 r_1, \quad \varepsilon_1\in\{\pm1\}, \quad 1\le r_1\le a-1\\
a &=& (2k_2)r_1+\varepsilon_2 r_2, \quad \varepsilon_2\in\{\pm1\}, \quad 1\le r_2\le r_1-1,\\
\ldots &=& \ldots\\
r_{\ell-2} &=& (2k_\ell)r_{\ell-1}+\varepsilon_\ell r_\ell, \quad \varepsilon_\ell\in\{\pm1\}, \quad r_\ell=1,
\end{array}$$

where $\ell:=\ell(a,p)$ is minimal with $r_\ell=1$. We show in the full paper that $\left(\frac{2^a+1}{2^p-1}\right)=(-1)^{\ell+1}$. We select the subset $\mathcal{A}(p)$ of odd a in the interval $[5,p-2]$ such that $\ell\equiv 0 \pmod 2$. We assume that there are a positive proportion of such, namely that there is a constant $c_1>0$ such that for large p, there are $>c_1p$ odd numbers $a\in[5,p-2]$ such that $\ell(a,p)\equiv 0 \pmod 2$. So, we have $\prod_{i=1}^k\left(\frac{2^a+1}{q_i}\right)=-1$ for $a\in\mathcal{A}(p)$. We next conjecture that for such a, the values are $\left(\left(\frac{2^a+1}{q_i}\right), 1\le i\le k\right)$ are uniformly distributed among the 2^k vectors $\underbrace{(\pm1,\pm1,\cdots,\pm1)}_{k\text{ times}}$. That is, $2^{a_i}+1$ is a quadratic residue modulo p_j for all $j\ne i$ but it is not a quadratic residue modulo q_i. In the full paper we provide an argument why we expect to find it and under the previous two conjectures the following should hold. The rest of our method is unconditional and we summarize it in the next algorithm.

Algorithm 1 works for most primes (and odd integers), and we applied it for $n\le 100$. But there are a few primes like 47 for which there is no $a_j\in[5,p-2]$ such that $\left(\frac{2^{a_j}+1}{q_i}\right)=(-1)^{\delta_{ij}}$, with Kronecker symbols as exponents. If that happens, the system may not be solvable (it has even determinant). However, experimentally, we observed that if it fails, we can always get suitable a_i's such that the corresponding matrix has odd determinant, and is therefore invertible. The factorization of 2^n-2 with weight 2 factors for odd $33\le n\le 100$ is given in Table 1.

Algorithm 1:

for *prime (or odd)* $p \leq B$ *(suitable bound)* **do**

  Factor $2^p - 1 = q_1 \cdots q_k$, where q_i is prime for $1 \leq i \leq k$;

  for $j = 1$ *to* k **do**

    Find odd $a_j \in [5, p-2]$ such that the Legendre symbol $\left(\frac{2^{a_j}+1}{q_i}\right) = (-1)^{\delta_{ij}}$ where δ_{ij} is the Kronecker symbol.

  end

  Take a primitive root ρ_i modulo q_i for $1 \leq i \leq k$;

  Find b_{ij} such that $2^{a_i} + 1 = \rho_j^{b_{ij}} \pmod{q_j}$ for $1 \leq i, j \leq k$;

  Find largest α_i such that 2^{α_i} is a divisior of $q_i - 1$ for $1 \leq i \leq k$;

  Calculate $\alpha = \max\{\alpha_i : 1 \leq i \leq k\}$;

  Solve the system of linear equations $\sum_{i=1}^{k} y_i b_{ij} = 2^{\alpha_j - 1}$ for $j = 1, 2, \ldots, k$. in $\mathbb{Z}_\alpha$

end

References

[1] L. Carlitz, "Permutations in a finite field", *Proc. Amer. Math. Soc.* **4** (1953), 538.

[2] R. T. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, **90**. Cambridge University Press, Cambridge, 1988.

[3] A. Kontorovich and J. Lagarias, "On toric orbits in the affine sieve", *Exp. Math.* **30** (2021), 575–587.

[4] F. Luca and P. Stănică, "Prime divisors of Lucas sequences and a conjecture of Skałba", *Int. J. Number Theory* **1** (2005), no. 4, 583–591.

[5] P. Mihăilescu, Preda (2004), "Primary Cyclotomic Units and a Proof of Catalan's Conjecture", J. Reine Angew. Math. **572** (2004), 167–195.

[6] P. Moree, "On the divisors of $a^k + b^k$", *Acta Arith.* LXXX.3 (1997), 197–212.

[7] L. Murata and C. Pomerance, "On the largest prime factor of a Mersenne number", in *Number Theory*, 209–218, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004.

[8] S. Nicoka, V. Nikov, V. Rijmen, "Decomposition of permutations in a finite field", *Cryptogr. Commun.* **11** (2019), 379–384.

[9] G. Petrides, "On decompositions of permutation polynomials into quadratic and cubic power permutations", *Cryptogr. Commun.* **15** (2023), 199–207.

[10] A. Rotkiewicz, "Applications of Jacobi's symbol to Lehmer's numbers", *Acta Arith.* **42** (1983), 163–187.

Table 1: Factorization of $2^n - 2 \pmod{2^n - 1}$ for odd $33 \le n \le 99$.

$n = 33$	$(2^5+1)^{599478} \cdot (2^{13}+1)^{299739} \cdot (2^{29}+1)^{1798434}$
$n = 35$	$\big((2+1)(2^{17}+1)\big)^{967995} \cdot (2^{29}+1)^{276570}$
$n = 37$	$(2^5+1)^{77039772} \cdot (2^{13}+1)^{19259943}$
$n = 39$	$\big((2^{11}+1)(2^{21}+1)\big)^{1592955}$
$n = 41$	$(2^9+1)^{20111512782} \cdot (2^{13}+1)^{3351918797}$
$n = 43$	$\big((2^5+1)(2^{17}+1)(2^{23}+1)\big)^{593211015}$
$n = 45$	$(2+1)^{407925} \cdot (2^{13}+1)^{349650} \cdot \big((2^{25}+1)(2^{33}+1)(2^{41}+1)\big)^{116550}$
$n = 47$	$(2^{11}+1)^{1927501725} \cdot (2^{37}+1)^{435242325} \cdot (2^{41}+1)^{1616614350}$
$n = 49$	$(2^9+1)^{34630287489} \cdot (2^{11}+1)^{3393768173922}$
$n = 51$	$(1+2^{29})^{150009615}$
$n = 53$	$(1+2^5)^{6512186850} \cdot (1+2^{15})^{3506562150} \cdot (1+2^{21})^{250468725}$
$n = 55$	$(1+2)^{6588945} \cdot (1+2^{11})^{5856840} \cdot (1+2^{17})^{732105}$ $\cdot (1+2^{25})^{1464210} \cdot (1+2^{33})^{10249470} \cdot (1+2^{47})^{732105}$
$n = 57$	$(1+2^5)^{396029391534} \cdot (1+2^{17})^{1188088174602} \cdot (1+2^{21})^{594044087301}$ $\cdot (1+2^{47})^{198014695767}$
$n = 59$	$(1+2^7)^{3663925098759300} \cdot (1+2^{13})^{305327091563275}$
$n = 61$	$(1+2^9)^{1152921504606846975}$
$n = 63$	$(1+2)^{42958503} \cdot (1+2^5)^{3735522} \cdot (1+2^{39})^{56032830} \cdot$ $(1+2^{43})^{44826264} \cdot (1+2^{47})^{29884176}$
$n = 65$	$(1+2^{17})^{72647571779055} \cdot (1+2^{23})^{72647571779055} \cdot (1+2^{29})^{72647571779055}$
$n = 67$	$(1+2^5)^{15295807610659665}$
$n = 69$	$(1+2^{11})^{36566619637113225} \cdot (1+2^{17})^{2437774642474215} \cdot$ $(1+2^{53})^{19502197139793720} \cdot (1+2^{67})^{21939971782267935}$
$n = 71$	$(1+2^{11})^{3659326099961865} \cdot (1+2^{13})^{14637304399847460}$
$n = 73$	$(1+2^{31})^{1726845200475585} \cdot (1+2^{45})^{107064402429486270}$
$n = 75$	$(1+2)^{36654975} \cdot (1+2^{39})^{17832150} \cdot (1+2^{41})^{9906750} \cdot$ $(1+2^{43})^{7925400} \cdot (1+2^{53})^{57459150} \cdot (1+2^{55})^{15850800} \cdot (1+2^{63})^{43589700}$
$n = 77$	$(1+2^{25})^{290641821624556479} \cdot (1+2^{31})^{290641821624556479} \cdot$ $(1+2^{41})^{290641821624556479} \cdot (1+2^{67})^{581283643249112958}$
$n = 79$	$(1+2^9)^{12102186118644337359} \cdot (1+2^{15})^{12102186118644337359} \cdot$ $(1+2^{41})^{12102186118644337359}$
$n = 81$	$(1+2)^{106331083505919} \cdot (1+2^{25})^{155626336778778} \cdot (1+2^{37})^{105108887143782} \cdot$ $(1+2^{39})^{155626336778778} \cdot (1+2^{43})^{4073987873790}$
$n = 83$	$(1+2^{11})^{7239076764159456135965}$
$n = 85$	$(1+2^9)^{4760486403166879215} \cdot (1+2^{13})^{4760486403166879215} \cdot$ $(1+2^{23})^{4760486403166879215}$
$n = 87$	$(1+2^{39})^{3371346107168004} \cdot (1+2^{41})^{280945508930667} \cdot (1+2^{53})^{2809455089306670} \cdot$ $(1+2^{61})^{4214182633960005} \cdot (1+2^{71})^{1685673053584002} \cdot (1+2^{83})^{280945508930667}$
$n = 89$	$(1+2^{13})^{30948500982134506872478105}$
$n = 91$	$(1+2^{59})^{280368506850705} \cdot (1+2^{67})^{1682211041104230} \cdot (1+2^{71})^{280368506850705} \cdot$ $(1+2^{73})^{280368506850705} \cdot (1+2^{81})^{3364422082208460}$
$n = 93$	$(1+2^{17})^{2305843010287435773}$
$n = 95$	$(1+2^{43})^{7354378117756963125} \cdot (1+2^{51})^{7354378117756963125}$
$n = 97$	$(1+2^5)^{61253537018541048982516284} \cdot (1+2^9)^{10208922836423508163752714}$
$n = 99$	$(1+2)^{160190876329840719} \cdot (1+2^{23})^{160190876329840719} \cdot (1+2^{35})^{58251227756305716} \cdot$ $(1+2^{57})^{29125613878152858} \cdot (1+2^{59})^{101939648573535003} \cdot (1+2^{75})^{58251227756305716}$